auser
Associazione
per l'invecchiamento attivo

Il *data breach*

Avv.
Paola Brillanti

Team Responsabile della Protezione dei Dati dell'AUSER

auser
Associazione
per l'invecchiamento attivo

Il «*data breach*»

- **È un evento, accidentale o volontario, che comporta la potenziale violazione della «*privacy*» degli interessati. Esempi di *data breach***: accesso o acquisizione dei dati da parte di terzi non autorizzati, furto o perdita di dispositivi informatici contenenti dati, deliberata alterazione di dati, impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (virus, *malware*, ecc.), perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità, divulgazione non autorizzata dei dati personali.
- **Ogni operatore autorizzato** a trattare dati (personale autorizzato), qualora venga a conoscenza di un potenziale caso di *data breach*, è tenuto ad **avvisare tempestivamente**, e comunque, **entro tre ore** da quando ne è venuto a conoscenza il **Presidente della propria Struttura AUSER di riferimento** il quale avvisa immediatamente il DPO (**privacy@auser.it**).

auser
Associazione
per l'invecchiamento attivo

rché è necessario avvisare in caso di «*data breach*»?

La segnalazione è necessaria, e deve essere immediata, perché il *data breach*

- deve essere registrato nel «Registro *Data Breach*» (è un registro informatico predisposto, aggiornato e conservato dal DPO per il Titolare del trattamento).

- deve essere notificato al Garante»: il titolare del trattamento deve effettuare la notifica al Garante privacy **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica venga effettuata **oltre le 72 ore, deve essere corredata dei motivi del ritardo**.

- deve essere comunicato agli interessati»: quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato **senza ingiustificato ritardo**. La comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione e **contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento UE 2016/679**.

auser
Associazione
per l'invecchiamento attivo

Furto o smarrimento del cellulare

Quando un operatore perde il proprio cellulare su cui aveva salvato la posta elettronica dell'AUSER o anche solo i numeri di cellulare di colleghi e/o di associati/persone assistite dall'AUSER, lo stesso operatore, oltre a seguire le indicazioni presenti nella *Policy Data Breach*, deve chiedere immediatamente alla struttura AUSER e, se necessario, al tecnico informatico di riferimento:

- **IL BLOCCO DELLA SIM DEL CELLULARE**
- **IL BLOCCO DEL CODICE IMEI DEL CELLULARE**

Questa duplice operazione, quando avviene in tempi molto ravvicinati rispetto al momento del furto e/o della perdita, ha una molteplice valenza: protegge i dati personali presenti sul dispositivo, protegge i diritti degli interessati sulla liceità della circolazione dei loro dati personali e facilita le operazioni necessarie per registrare la violazione e decidere se procedere o meno alla notifica e alla comunicazione agli interessati.

auser
Associazione
per l'invecchiamento attivo

Furto o smarrimento del cellulare
Come gestire la segnalazione

Cosa fare quando un operatore segnala di aver perso il telefono per furto o vero e proprio smarrimento:

1. **Verificare** se ha già esposto denuncia e cosa è stato scritto nella **denuncia**.
2. **Verificare se il cellulare era protetto** (es. pin/*password*/riconoscimento volto blocco schermo) e **fare una ricognizione dei dati personali presenti nel telefono** (es. rubrica telefonica, posta elettronica, allegati scaricati…).
3. Se era già stata fatta la denuncia, **procedere, ENTRO POCHE ORE (24-72) dal momento della segnalazione dell'operatore, alla richiesta di blocco della sim e del codice IMEI presso l'operatore telefonico**. Se non era già stata fatta la denuncia, effettuate la denuncia e CONTESTUALMENTE/IMMEDIATAMENTE DOPO la richiesta di blocco della sim e del codice IMEI presso l'operatore telefonico.
4. **Cambiare la password di accesso alla casella di posta elettronica** dell'operatore che ha perso il dispositivo.
5. OGNI VOLTA CHE è POSSIBILE **FORMATTARE IL CELLULARE DA REMOTO** SEGUENDO LE ISTRUZIONI **ANDROID** (https://support.google.com/nexus/answer/6160491?hl=it) ED **APPLE** (https://support.apple.com/it-it/guide/icloud/mmfc0ef36f/icloud).
6. **Scrivere al DPO (privacy@auser.it) il riassunto di tutti i punti sopra indicati allegando la denuncia e la richiesta di blocco all'operatore telefonico**.

auser
Associazione
per l'invecchiamento attivo

Alcuni *data breach*…

- **FURTO DI UN DISPOSITIVO (UN PC)** utilizzato da un operatore autorizzato: l'operatore aveva salvato le pratiche sul *desktop*. **Conseguenze**: notifica al Garante e invio di un centinaio di racc. a.r. agli interessati.
- **UTILIZZO DI SITI, APPLICAZIONI E APERTURA DI LINK NON VERIFICATI DALL'ADS** contenenti *virus*, *malware* e altri contenuti malevoli in grado di leggere la posta elettronica e i dati personali presenti nei dispositivi. **Conseguenze**: notifica al Garante e pubblicazione di avviso sul sito della struttura.
- **SMARRIMENTO DI TESSERE** da parte di un operatore autorizzato in seguito al furto della borsa/dello zaino contenente le tessere. **Conseguenze**: notifica al Garante e invio di racc. a.r. agli interessati.
- **INVIO DELLA TESSERA**, a mezzo PEC **AD UNA MOLTITUDINE DI SOGGETTI TERZI NON AUTORIZZATI**: errore umano. **Conseguenze**: notifica al Garante e invio di racc. a.r. all'interessato.
- **INVIO DI E-MAIL MASSIVE A 4.000 INDIRIZZI IN COPIA CONOSCENZA** (cc) e non in copia conoscenza nascosta (ccn): errore umano. **Conseguenze**: notifica al Garante e comunicazione agli interessati tramite e-mail.
- **APERTURA DI E-MAIL DI *PHISHING*** che richiedeva con urgenza di cambiare la *password*. In seguito la casella di posta elettronica ha iniziato a inviare e-mail di *phishing* ad un indirizzario parzialmente non noto alla struttura: errore umano. **Conseguenze**: notifica al Garante e pubblicazione di avviso sul sito della struttura.

auser
Associazione
per l'invecchiamento attivo

...come evitare le conseguenze

1) **FURTO DI UN DISPOSITIVO (PC):** salvare tutti i documenti **sul cloud e non in locale (sul desktop)**; **chiedere all'amministratore di sistema di criptare l'*hard disk* del pc**.
2) **UTILIZZO DI SITI, APPLICAZIONI E APERTURA DI LINK NON VERIFICATI DALL'ADS: chiedere all'amministratore di sistema** se l'applicazione che si vuole scaricare è sicura.
3) **SMARRIMENTO DI CHIAVETTE USB: prima di usare la chiavetta chiedere all'amministratore di sistema di criptarla con *password*.**
4) **INVIO TRAMITE E-MAIL DI DOCUMENTI CONTENENTI DATI SENSIBILI A PERSONE NON AUTORIZZATE:** inviare gli allegati all'interno di **cartelle zip criptate** oppure seguendo le istruzioni per condividere i file **tramite il cloud** e **comunicare le password per scaricare i documenti mediante un canale diverso dalla mail** (es. tramite telefono).
5) **INVIO DI E-MAIL MASSIVE: inserire i destinatari in ccn/bcc** (ultimo campo compilazione mail)
6) **APERTURA DI E-MAIL DI PHISHING:** ogni volta che si riceve una **e-mail** che chiede **conferma o rinnovo di *account/password*, non cliccare nulla e segnalare la mail all'amministratore di sistema. ATTENZIONE: il Garante privacy ritiene molto importante svolgere test e corsi di formazione in tema di phishing e cybersicurezza (https://www.garanteprivacy.it/temi/cybersecurity)**

auser
Associazione
per l'invecchiamento attivo

...le conseguenze possono comportare SANZIONI

La violazione degli obblighi previsti dalla normativa comporta l'irrogazione di una sanzione amministrativa fino a 20 milioni di euro.

La violazione degli obblighi fa sorgere a carico dell'AUSER responsabilità CIVILE (l'interessato può chiedere i danni).

In ogni caso di violazione della normativa privacy il Garante può disporre la «limitazione» o il divieto del trattamento.

auser
Associazione
per l'invecchiamento attivo

Grazie per l'attenzione

Avv.
Paola Brillanti

Team Responsabile della Protezione dei Dati dell'AUSER

privacy@auser.it